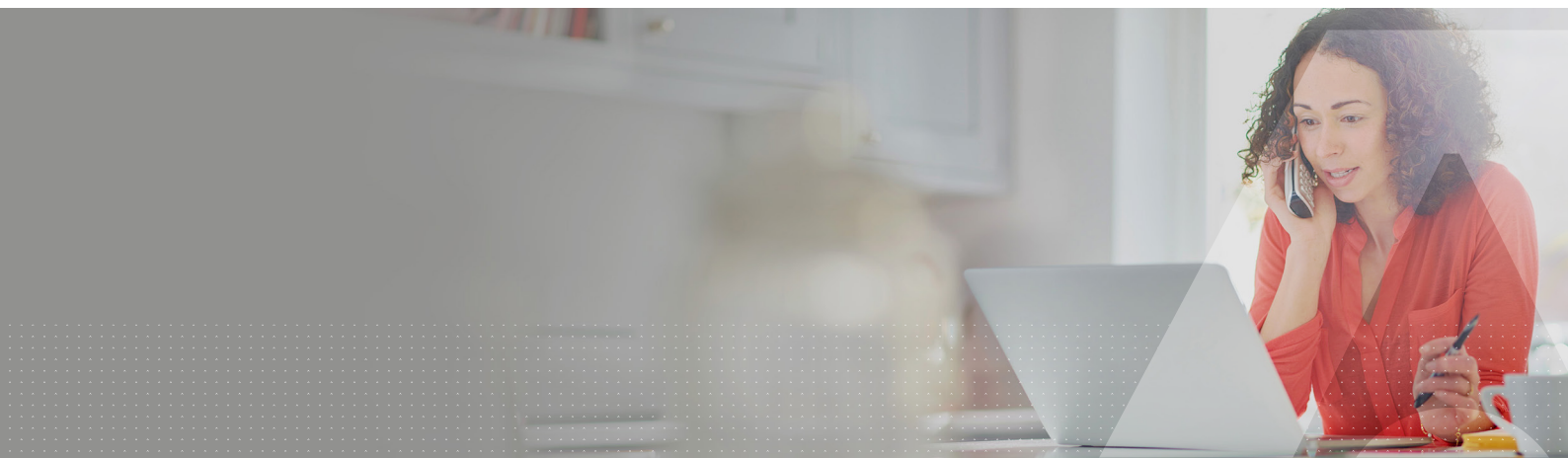


Dispositivos sin contraseña SafeNet FIDO2

Disminuya el riesgo de brechas de seguridad con la autenticación de múltiples factores sin contraseña



Las organizaciones que vienen expandiendo su transformación digital desplazan aplicaciones y datos a la nube para (1) permitir la accesibilidad desde cualquier lugar y (2) disminuir los costos operativos. A medida que los usuarios inician sesión en un número cada vez mayor de aplicaciones basadas en la nube, las contraseñas débiles emergen como la principal causa del robo de identidades y las brechas de seguridad.

Para reducir el riesgo asociado con su inicio de sesión de Windows, las aplicaciones SaaS, los usuarios con altos privilegios y los usuarios en general, Thales es compatible con la autenticación sin contraseña FIDO mediante dispositivos de hardware de autenticación de múltiples factores (MFA).

Reemplazar las contraseñas con el hardware del autenticador FIDO ofrece una experiencia moderna de MFA sin contraseña que es resistente a los ataques de phishing y la apropiación de cuentas, además de permitir el cumplimiento.

Los dispositivos de autenticación de múltiples factores de Thales utilizan protocolos actuales y emergentes para admitir múltiples aplicaciones al mismo tiempo. Utilice una clave que combine la compatibilidad con FIDO2, WebAuthn, U2F y PKI para acceder tanto a espacios físicos como a recursos lógicos.

Autenticación sin contraseña FIDO2

La autenticación FIDO sin contraseña reduce el riesgo de brechas de seguridad al reemplazar las contraseñas textuales vulnerables con la autenticación FIDO.

La autenticación FIDO ha ganado fuerza como una forma moderna de MFA debido a sus considerables beneficios al facilitar la experiencia de inicio de sesión para los usuarios y superar las vulnerabilidades inherentes de las contraseñas basadas en texto. Las ventajas incluyen menos fricción para los usuarios y un alto nivel de seguridad.

Habilite recorridos de autenticación de múltiples usuarios

Thales, el líder mundial en seguridad digital, admite numerosos métodos de autenticación sin contraseña con una poderosa gama de dispositivos FIDO



FIDO con tarjeta convergente

Acceso físico: Para una comodidad óptima, las tarjetas inteligentes FIDO de Thales admiten el acceso físico, lo que les permite a los usuarios acceder tanto a espacios físicos como a recursos lógicos con una única tarjeta inteligente personalizable.

Amplíe la autenticación moderna a entornos PKI: Las organizaciones que dependen de la autenticación PKI ahora pueden usar una tarjeta inteligente combinada PKI-FIDO para facilitar sus iniciativas de transformación digital y en la nube al proporcionar a sus usuarios un único dispositivo de autenticación para asegurar el acceso a aplicaciones heredadas, dominios de red y servicios en la nube.

Acceso remoto

Ya sea que trabajen desde casa o mientras viajan, los usuarios pueden iniciar sesión en aplicaciones corporativas basadas en la nube desde múltiples dispositivos en múltiples ubicaciones.

Los autenticadores FIDO de Thales brindan acceso remoto seguro con MFA para proteger su organización independientemente del dispositivo de punto final y la ubicación.

Inicio de sesión en red y PC con Windows

Los autenticadores FIDO proporcionan MFA sin contraseña, lo que permite a los usuarios acceder de forma segura a PC y tabletas con Windows. Con las tarjetas FIDO PKI combinadas, podemos ofrecer un solo dispositivo para iniciar sesión de forma segura en cualquier sistema operativo, incluidos Windows 10, 8 y 7, Windows Server OS, macOS y Linux. Esto significa que las organizaciones pueden utilizar dispositivos Thales FIDO-PKI para soportar sus necesidades de autenticación y firma digital FIDO y PKI.

Proteja las aplicaciones SaaS

Dado que la mayoría de los usuarios reutilizan sus contraseñas en todas las aplicaciones, puede mejorar la seguridad drásticamente y reducir las llamadas al servicio de asistencia al equipar a los usuarios con autenticadores FIDO. Los dispositivos FIDO de Thales son totalmente compatibles con Azure AD y garantizan un acceso seguro a las aplicaciones administradas de Azure AD.

Acceso móvil seguro

Los dispositivos FIDO de Thales apoyan la autenticación moderna en cualquier dispositivo al permitir que los usuarios se autenticen sin contacto con un método de tipo "tap & go" para obtener acceso seguro a cualquier recurso en la nube desde cualquier dispositivo móvil.

Gestión de acceso privilegiado

Los usuarios con acceso a información privilegiada con permisos elevados o la capacidad de iniciar sesión en soluciones PAM tienen acceso inmediato a datos confidenciales: sus cuentas son el objetivo final de los hackers.

Proporcionarles autenticación de múltiples factores a los usuarios con acceso privilegiado para reemplazar las contraseñas vulnerables, garantiza que solo los usuarios autorizados puedan acceder a los recursos privilegiados.

Compatibilidad con los IDP

Los dispositivos sin contraseña SafeNet FIDO2 son compatibles con cualquier proveedor de identidad (IDP) que admita el estándar FIDO2.

Consulte nuestro sitio web para obtener una lista de los desplazados internos con los que hemos realizado pruebas y validaciones en conjunto, en <https://cpl.thalesgroup.com/access-management/authenticators/fido-devices>

Para todas las empresas, ofrezca a sus empleados y contratistas un único dispositivo para todas sus necesidades de autenticación y acceso, ya sea que trabajen desde casa o en la oficina. Permita el acceso físico a los edificios y áreas controladas y facilite la movilidad de los empleados. Considere sus casos de uso y elija entre los autenticadores SafeNet FIDO.

Características del producto	SafeNet IDPrime 3940 FIDO	SafeNet eToken FIDO	SafeNet IDCore 3121 FIDO	SafeNet IDPrime 941 FIDO	SafeNet IDPrime 931 FIDO
Factor de forma	Tarjeta inteligente	Token USB-A	Tarjeta inteligente	Tarjeta inteligente	Tarjeta inteligente
Contacto (ISO 7816)	FIDO y PKI	N/A	N/A	PKI	PKI
Sin contacto (ISO14443)	FIDO y PKI	N/A	FIDO y Acceso físico	FIDO y Acceso físico	FIDO y Acceso físico
Memoria					
Chip de memoria	400 KB Java Flash	400 KB Java Flash	586 KB de ROM de usuario	Chip de contacto: 400 KB Java Flash Chip sin contacto: 586 KB ROM de usuario	Chip de contacto: 400 KB Java Flash vChip sin contacto: 586 KB ROM de usuario
Memoria libre disponible para claves residentes, certificados, subprogramas y datos adicionales	73 KB	90 KB	88.3 – 98.3 KB	Contacto: 73 KB Sin contacto: 88.3 – 98.3KB	Contacto: 73 KB Sin contacto: 88.3 – 98.3KB
Capacidad de claves					
Claves de residente FIDO	Hasta 8	Hasta 8	Hasta 8	Hasta 8	Hasta 8
Contenedores de claves PKI	20	N/A	N/A	20	20
Estándares compatibles					
Java Card	3.0.4	3.0.4	N/A	3.0.4	3.0.5
Global Platform 2.2.1	✓	✓	N/A	✓	✓
FIDO 2.0	✓	✓	✓	✓	✓
U2F	✓	✓	✓	✓	✓
Minicontrolador CSP base (minicontrolador SafeNet)	✓	N/A	N/A	✓	✓
Algoritmos criptográficos (PKI)					
Hash: SHA-1, SHA-256, SHA-384, SHA-512.	✓	N/A	N/A	✓	✓
RSA: Hasta RSA 4096 bits	✓	N/A	N/A	✓	✓
RSA OAEP y RSA PSS	✓	N/A	N/A	✓	✓
P-256 bits ECDSA, ECDH. P-384 y P-521 bits ECDSA, ECDH están disponibles mediante una configuración personalizada	✓	N/A	N/A	✓	✓
Generación de pares de claves asimétricas en la tarjeta (RSA hasta 4096 bits y curvas elípticas hasta 521 bits)	✓	N/A	N/A	✓	✓
Simétrico: AES: para mensajería segura y 3DES solo para desafío/respuesta de Microsoft	✓	N/A	N/A	✓	✓

Características del producto	SafeNet IDPrime 3940 FIDO	SafeNet eToken FIDO	SafeNet IDCore 3121 FIDO	SafeNet IDPrime 941 FIDO	SafeNet IDPrime 931 FIDO
Certificaciones					
Chip: CC EAL6+	✓	✓	N/A	✓	✓
Certificación NIST: FIPS 140-2 N2	N/A	N/A	N/A	N/A	✓
Plataforma Java: tarjeta CC EAL5 +/PP certificada por java	✓	✓	N/A	✓	N/A
Plataforma Java + aplicativo de PKI: CC EAL5+/PP QSCD	✓	N/A	N/A	✓	N/A
Calificación de eIDAS para eSignature y eSeal	✓	N/A	N/A	✓	N/A
ANSSI de Francia	✓	N/A	N/A	✓	N/A
Acceso físico: configuraciones Mifare Classic y DesFire	N/A	N/A	✓	✓	✓
Otras características					
Política de PIN a bordo	✓	N/A	N/A	✓	✓
Compatibilidad con PIN múltiples	✓	N/A	N/A	✓	✓
Personalización y branding	✓	N/A	N/A	✓	✓
Sistemas operativos					
FIDO compatible con Windows 10 y otros sistemas operativos compatibles con FIDO	✓	✓	✓	✓	✓
PKI compatible con Windows, macOS X y Linux	✓	N/A	N/A	✓	✓

Acerca de las soluciones de autenticación y gestión de acceso SafeNet de Thales

Las soluciones de autenticación y gestión de acceso líderes en la industria de Thales les permiten a las empresas administrar de manera centralizada y proteger el acceso a las aplicaciones empresariales de TI, basadas en la web y en la nube. Mediante el uso de SSO basados en políticas y métodos de autenticación universal, las empresas pueden prevenir infracciones de forma eficaz, migrar a la nube de forma segura y simplificar el cumplimiento normativo.

Acerca de Thales

Las personas en las que confía para la protección de su privacidad confían en Thales para proteger sus datos. Las empresas se enfrentan a un número cada vez mayor de momentos decisivos relacionados con la seguridad de los datos. Tanto si se trata de elaborar una estrategia de cifrado, como de migrar a la nube o de cumplir los requisitos normativos, puede confiar en Thales para proteger su proceso de transformación digital.

Tecnología decisiva para momentos decisivos.